5-2014

Mobile Banking Security Using GPS and LDPC Codes

Matthew Francis Moccaro
University of Arkansas, Fayetteville

Mobile Banking Security Using GPS and LDPC Codes

Mobile Banking Security Using GPS and LDPC Codes

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Science in Computer Engineering

by

Matthew Moccaro
Rutgers University
Bachelor of Science in Computer Engineering, 2012

May 2014
University of Arkansas

This thesis is approved for recommendation to the Graduate Council.

_____
Dale R. Thompson, Ph.D., P.E.
Thesis Director

_____
John Gauch, Ph.D.
Committee Member

_____
Craig Thompson, Ph.D.
Committee Member

ABSTRACT

Mobile Banking is becoming a major part of our world's financial system. Being able to manage one's finances on a mobile device can provide services that can make users more productive. It can also serve as a means of financial freedom to those who are unable to access physical banking facilities due to distance, or other problems. However, with such freedom also comes the need for security. A person's financial information is one of the most targeted groups of information by attackers. To secure these mobile freedoms, this paper presents a system to secure mobile banking procedures using global positioning systems (GPS) within mobile devices, and low density parity codes (LDPC). The approach is to determine a user's daily locations, set them as trusted locations, and use LDPC codes not only to obscure this data from attackers, but to help in correcting inaccurate GPS readings. The conclusions, based on thorough testing, is that this system is able to more readily secure a person's mobile banking applications on their mobile device.

ACKNOWLEDGEMENTS

I thank Dr. Dale R. Thompson for his assistance and guidance throughout my time at the University of Arkansas. I also thank Drs. John Gauch and Craig Thompson for reviewing this thesis and for all of their help throughout the last several years.

I also thank my family, friends and colleagues who have supported me throughout my time at the University of Arkansas.

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION

A. MOTIVATION

Mobile solutions are becoming an increasingly important part of society. They can help to make us more efficient and help to keep us connected to our families and to our careers. Mobile solutions can also help us to perform tasks we would not normally be able to perform. They can give resources to those who would otherwise be without them. One of the indispensable resources of modern societies is that of a banking system. Banking systems have helped many societies grow and flourish monetarily while helping residents to lead better lives and to manage their money in a productive way. However, an established banking system may not always be available or feasible to residents in all countries. This is a perfect example of a problem that can be solved with today's innovative mobile solutions. By creating a system of mobile banking, we can help to bring the benefits of a banking system to those who would, under normal circumstances, have no access to banking facilities. However, this system would be useless without the promise of a secure user experience. Making the system secure against attacks and keeping users' financial information safe is critical for a stable banking system. Together, we can see the importance of bringing a secure mobile banking system to those who cannot normally be afforded this opportunity.

The importance of bringing a secure mobile banking system to users can be illustrated with several examples. One of the most prominent examples can be seen in the country of Kenya, where a mobile banking system named M-Pesa has helped many citizens to gain access to the mobile banking facilities they need in their daily lives [1]. Research conducted regarding this project has shown that the distance between an individual and their banking facilities is a major constraint. If there is a great distance between a resident and the nearest banking facility,

the cost of traveling to and from the facilities may not be worth the services offered. However, M-Pesa in Kenya is able to eliminate this inconvenience and allow users to experience banking as if the facilities were close by. Companies also benefitted from the system, as they were able to use M-Pesa to pay their employee's salaries and to collect bill payments from customers. Without a mobile banking solution, none of these things would be possible, which illustrates how important the M-Pesa system is to its users.

Without a mobile banking solution, many places, such as Kenya, may not be able to give their citizens access to mobile banking facilities for a large amount of time. Implementing actual banking facilities within a region requires that an infrastructure be established to allow citizens to travel to these facilities. However, the terrain in some regions of the world may make establishing this infrastructure, such as building roads and establishing necessary resources such as power lines, very difficult. Also, without strong techniques to secure these solutions, the users will not use them, and therefore they will be rendered useless. A person's financial information is vital to their continued living, and losing it through an insecure system of mobile banking, no matter how great the services are, is never worth the risk.

B. OBJECTIVE

The objective of this work is to authenticate a user of a mobile banking application by location in addition to a username-password combination while obscuring and correcting the secure locations with LDPC codes. This enhanced security can lead to a more secure mobile banking experience that requires no new hardware modifications.

C. APPROACH

To create a mobile banking system that is both useable and secure, it is proposed to use GPS positioning as an additional form of user authentication. GPS positioning can be added to an application with the use of "trusted locations." Since a user is normally located within the same several regions each day, it is proposed that a user can set these locations as trusted locations. Once set, the banking application can be used at these locations with the added security of knowing that the user is in a location where they normally would be. If the phone is stolen or attacked, the attacker will not be able to use the mobile banking application outside of the trusted locations without additional credential verification such as a username and password.

Low density parity check (LDPC) codes are used in this system to enhance security and location privacy. These codes are normally used to correct errors in a bit stream. However, they can also be used to correct inaccurate GPS readings, and help to obscure GPS coordinates when stored in a database. These codes and their usage are explained in detail later.

D. ORGANIZATION OF THE THESIS

Chapter 2 describes the GPS system, LDPC codes, mobile banking security, and location privacy. The designs of the system and the prototype are described in Chapter 3. Chapter 4 describes experimental GPS accuracy and prototype testing results. Finally, Chapter 5 discusses the conclusions drawn about this approach and how viable it is for deployment.

II. BACKGROUND

A. INTRODUCTION

The following concepts are key to understanding this work. Global Positioning System (GPS) is used to validate the user is described. Low density parity check codes, or LDPC codes, aid in the system's accuracy and privacy concerns. Location privacy is defined as this is crucial to the system's desirability. Finally, the advantages and security challenges of mobile banking are discussed.

GPS

The Global Positioning System is a system of satellites used for navigation and other purposes [2]. It was originally built by the U.S. Department of Defense who placed twenty-four satellites into orbit and had originally intended them for military purposes only. The first of these satellites was launched in 1978 and the last in 1994, but replacements have been launched ever since due to maintenance. With time, the system was made available for civilians to use as well. It is a free system available to those with a GPS receiver and can help a person find their exact location on earth.

To use the GPS system, a person must have a GPS receiver. GPS receivers determine a person's location through the technique of trilateration [3]. A receiver will first find and lock on to, at least, three satellites. After this process is completed, the receiver will then measure the time it takes to send a signal from the receiver to the satellite. This will allow the receiver to determine the distance between itself and the satellite that it has locked on to. After completing this process with three satellites, the receiver is able to perform some elaborate calculations in order to determine its location. These calculations include those done to correct errors, which

can occur due to many factors in the environment including delays in the ionosphere. Other sources of errors for GPS signals include tall buildings or large rock surfaces [2], which cause a signal to reflect off of these objects before it reaches the receiver. This is called a signal multipath error. Another common source of error is the number of satellites that are visible. GPS receivers normally do not work underground or inside buildings, as there signal reception will be blocked. However, most GPS receivers have an error of only a few meters, and are useful in a multitude of applications. GPS receivers are also relatively inexpensive, and are a popular form of navigation in today's modern world.

LDPC

Low Density Parity Check Codes, or LDPC codes, are error-correction codes used to correct errors that may occur in a stream of bits [4]. Robert Gallagher first proposed these codes in his Ph. D thesis, which was published in 1968. Initially, these codes were dismissed as the computational power required to perform the calculations involved was, at the time, completely implausible. Over thirty years passed, and many researchers were unable to bridge the gap between theory and practice. However, in 1993, "turbo codes" were introduced into the field. These codes by Berrou, Glavieux, and Thitimajshima revolutionized this area [4]. With new interest came more research, and a short time later two researchers McKay and Neal rediscovered LDPC codes [4]. These codes were studied by many researchers who created LDPC codes that outperformed turbo codes. These codes have found use in many applications and look to have a bright future ahead of them [5]. Some example applications, which use LDPC codes are 10 Gigabit Ethernet, WiMAX, WiFi, and deep-space satellite missions.

The use of LDPC codes begins by taking a stream of bits of information, which is to be transferred through a noisy channel, one where bit stream errors are likely to occur. This information is then put into an encoder, which encodes the original bits of information with parity bits, creating a codeword. This codeword is then sent through the noisy channel, where bit errors may or may not occur. Finally, once the information reaches its destination, it is sent through an iterative decoder, which is able to not only determine how many bits are in error but also correct these bits as well. This property makes LDPC codes error-correcting codes. There are many different variants of LDPC codes that have different processes for encoding and decoding. All of these variants have different properties but all will follow this same high-level process of correcting bits in a stream prone to errors.

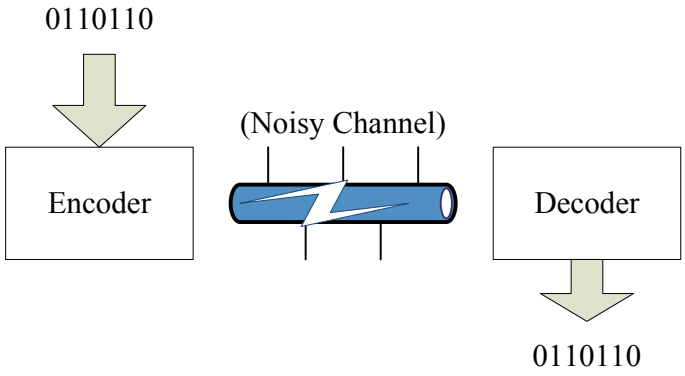

Figure 1. High-Level Diagram of Error Correction such as LDPC.

Location Privacy

Location privacy is a term which developed out of the popularity of location enabled devices and services [6]. New services and applications on today's smartphones allow users to track their location, share with others where they are or have been, and enhance social services. These applications share information to be effective. However, sharing one's location or having

location data stolen could have negative impacts such as someone unknown to you tracking your location to perform malicious acts, someone following you to these locations in order to steal your belongings when you are unaware, and an attacker using this location data to know when you are out of the house to rob you. This is the issue of location privacy, which becomes more prevalent with time, as location based systems on mobile devices become more accurate every day.

Mobile Banking

Mobile Banking is a term, which refers to the handling of banking affairs through a mobile device [7]. As mobile devices gained momentum in their usability and features, many technologies and services were developed for use with them. The banking sector was also quick to begin to develop its own solutions for mobile devices to attract users. Mobile banking has many benefits over others types, including no place restriction, high penetration coefficient, full personalization, and constant availability. With these advantages however, come many risks. When dealing with banking services, one is also dealing with one of their most important assets, their financial information. Therefore, great care must be taken to secure this information, yet still allow it to be usable for mobile banking services.

B. RELATED WORK

Mobile Banking Security

Mobile banking security is a crucial area to the continued success of mobile banking. Financial information is extremely sensitive information, which could have devastating results if stolen. Some examples of these results could be that a person could gain your financial information, and then transfer all of the funds out of your accounts into their own. Someone

could, once they have obtained your financial information, use this information to buy a highly priced item with your money. These are only two of the many catastrophic things that could happen if one's financial information is stolen.

One of the most popular areas of research is that of trying to improve the security of the protocols used between the communication points for mobile banking. Chang and Yang [8] developed a protocol to be used between a customer, merchant, and their respective banks. This protocol focused on security involving authentication via the mobile operator, or MO. Elkhodr and Shahrestani [9] also developed a new approach to secure a user's financial data by combining the Transport Layer Security (TLS) protocol with a newly implemented trust negotiation method, involving the mobile phone's IMEI and SIM serial number.

Besides protocol modification, many researchers have attempted to use biometric verification as well. Biometric verification involves using an individual user's personal information, such as a fingerprint scan, to verify and authenticate the user. In fact, using fingerprint scanners is one of the most popular areas of research. An example of this is Gordon and Sankaranarayanan [10], who constructed their own prototype system that included a mobile device with a supporting fingerprint scanner. This verification scheme only allowed the user to make mobile payments with the correct authentication. Another example of research, which involved the use of biometrics for mobile banking security, includes Chen and Zhuang [11], who combined biometric information with a one-time password (OTP).

Some research investigates inexpensive mobile banking security. Panjwani and Cutrell [12] developed a system in which all-mobile banking users are given codebooks. These codebooks are filled with a set of codes, which are used to log in. Each time a user logs into their mobile application, they use the next code in their codebook. When a user reaches the last

code, they return the book to the bank where it is disposed of and they are given a new set of codes for future use.

Finally, there is research on defining the threats and attacks to mobile banking. Michael Paik [13] describes several attacks on GSM systems including replay attacks, spoofing, and denial of service attacks. Cao and Fan [14] describe attacks including cross frame scripting and reflection injection. Both papers go on to describe ways to remedy these attacks and how to properly defend against them. Some of these defenses include authentication in the form of user authentication and device authentication, out-of-band authentication, second-factor authentication and others.

Location Privacy

Location privacy, another active research area, aims to protect the location identities of users everywhere. This issue has become important because mobile devices are capable of tracking an individual's location. Andersen, Kjaergaard and Gronbaek [6] developed the SITA principle for location privacy. This principal divided location privacy into four independent properties, which included spatial, identity, temporal, and activity (SITA) to try and cope with restrictions such as the on/off restriction. The on/off restriction is one in which the users tend to be biased towards disabling privacy, or turning it "off", due to the limitations imposed with privacy enabled. For example, spatial obfuscation may limit a user in the places where he or she may use an application. Therefore, users will probably tend to turn this privacy setting off. Another research project, Dewri [15], involved leveraging the current processing power of mobile devices, which he suggests are able to support the needs of location based services so that a minimal amount of location data is transferred out of the device, thereby minimizing the chances of this data being stolen and maliciously used. This is accomplished by the mobile

device itself performing a location-based point-of-interest search, therefore reducing its need on a third-party server.

Finally, Brassil and Manadhata [16] tried to prove a user's location based on femtocells. Femtocells are low-power access points that are used to connect a user's mobile device to their mobile operator. Femtocells also normally use public wired Internet access as backhaul, such as a connection to an AP. A user's location is proven by sending rate-controlled data traffic, which is used to impress a traffic signature at a specific femtocell. Therefore, when a user's device is receiving data at said femtocell, their location can be verified. Their system adds two things to a public Wi-Fi access point with an Internet connection including a femtocell, and a location server. The system can measure the bandwidth between the femtocell and the AP to verify location. For example, the bandwidth between an AP and a femtocell can be constantly monitored. If a party wants to verify a user's location, within a few seconds of initiating a transfer to the user, the party can expect to see an increase in the bandwidth values between that AP and the femtocell that is equivalent to the bandwidth values privately set by the party for their rate-controlled transmission. If there is not enough increase to convince the party that the user is actually within range of that femtocell, the party can decide that the user's location is not authenticated.

III. APPROACH

A. HIGH LEVEL DESIGN

The proposed solution to mobile banking security involves creating a system which uses trusted locations to help authenticate the user, while still maintaining location privacy. During the course of time, users are usually located in the certain places day after day. These places can be used to the advantage in this system, which would identify them as "trusted locations." These locations are obscured and stored in a database for future use. When a user tries to use the application at a later time, the application will measure the GPS coordinates and check if the user is within an acceptable range of the previously set "trusted location." If they are, the user is allowed to continue on and carry out banking transactions and procedures. If they are not within range, the user is asked a challenge question to prove their identity. If they are properly validated, the user can choose to set their current location as a trusted location for future use if they plan to be in that location often.

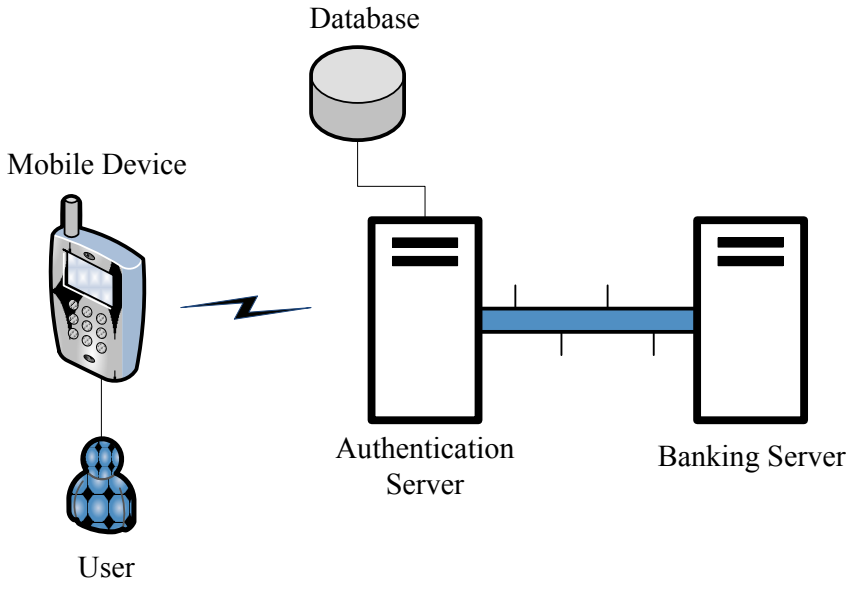

Figure 2. High-Level Overview of the System

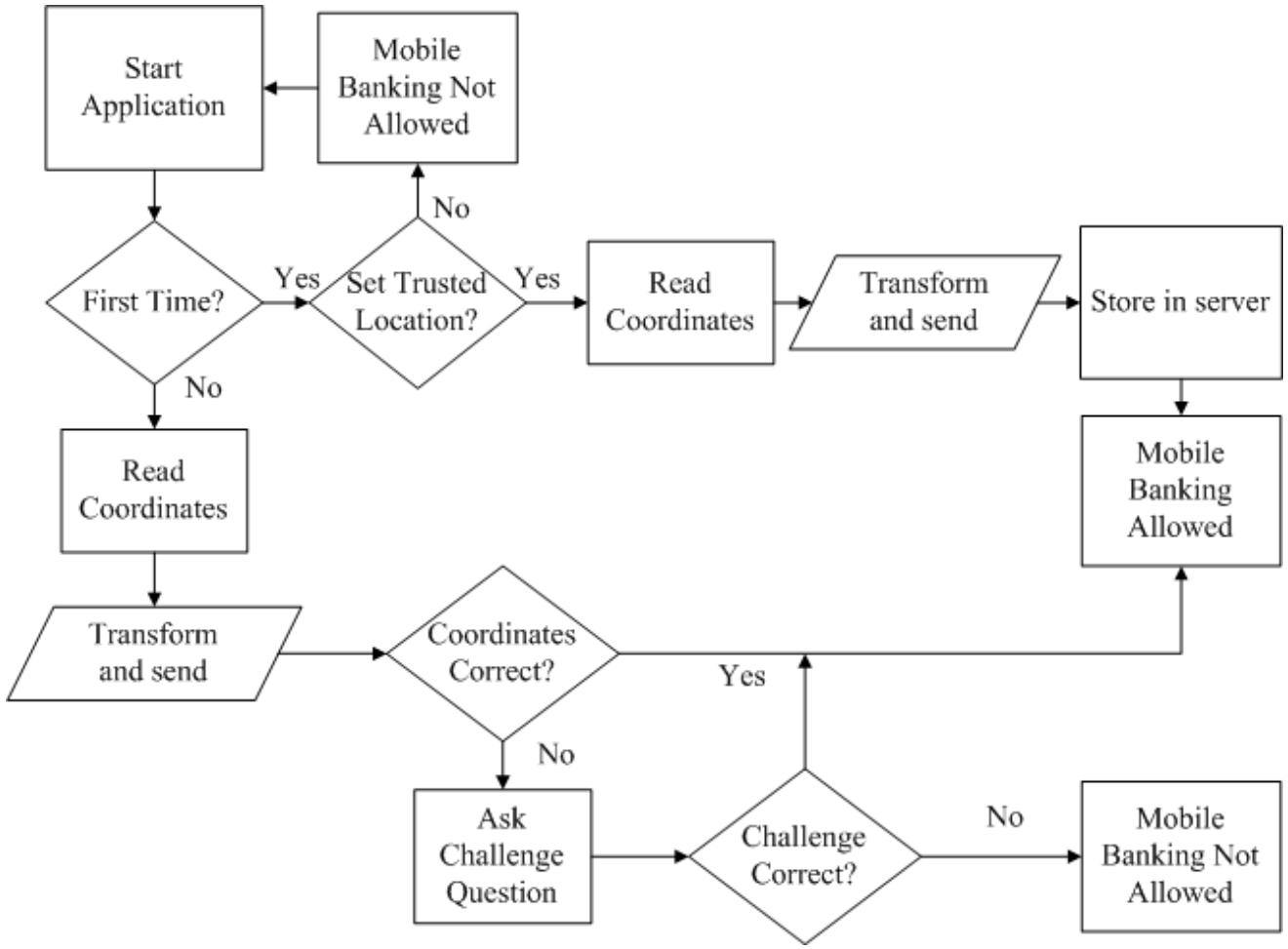

Figure 3. High-Level Overview Of GPS System

GPS and Trusted Coordinates

The basis for our solution is using a user's location to authenticate them. To do so, we must take GPS readings of the user's position each time they try to log in to the application. In this section, we present each step of the process in which this system builds a profile for the trusted locations of each user.

Our system is initiated the first time a user starts their mobile application. The application will first measure the GPS coordinates of the user using the equipped GPS sensors on the mobile device. These measurements are returned in the form of a number with up to fifteen decimal places. Since this is the user's first time running the application, the rest of the application may need to establish things such as usernames, passwords. The user will be asked if they want to set their current location as a "trusted location." This should be somewhere that the user is commonly found each day, and somewhere where the user feels they will need to use this application most frequently. If the user decides that the location is not to be set as a trusted location, the user will not be able to use the application. If they are in a place in which they feel is a trusted location, the phone will then properly transform the coordinate data and send the appropriate information to a server to be stored. This transformation will be explained in detail in the next section, section 3.1.2.

After the data is sent to the server, we now discuss the processes when a user tries to access the application a second time. When the user opens their application for a second time, the app immediately measures the GPS coordinates of its current position. It then transforms this data and sends it to the server, so that it can be determined whether or not the user is within an acceptable range of a trusted location. If the user is within range of their previously set trusted locations, they will be able to use their application as normal. This includes entering their

username and password and the application functioning as a typical mobile banking application would. If the user is not within range of a trusted location, several options can be put into effect. The first and simplest choice would be to ask the user a simple challenge question. If the user answers correctly, they can either temporarily use the application, or choose to set that location as a trusted location. Another option is to send the user an email for authentication in which they can click an acceptance link. This would force an attacker who was trying to use the phone outside of a trusted location to have also gained access to a user's email. This cycle continues for as long as the user uses the application, keeping the user's financial information safe while performing mobile banking operations, and keeping their location privacy intact.

LDPC Codes

Low density parity check codes are also a vital part of our system. They perform the tasks of maintaining location privacy by obscuring GPS coordinates, and correcting errors from inaccurate GPS readings. An overview of this process and its reasoning are explained below and shown in Figure 4.

When GPS readings are taken, they can sometimes be very inaccurate. These inaccurate readings can cause the proposed system not to function as expected. To remedy this problem, the use of LDPC codes was introduced into the system. LDPC codes are normally used to correct errors in a bit stream. For example, when a set of bits is sent over a noisy channel, some bits can be lost or changed when the set reaches its destination. LDPC codes can, within reason, detect which bits have been sent incorrectly and repair them to their original state. As described previously, this is done via an encoder and a decoder. In this system, these codes can be used much in the same way. However, instead of correcting bits in a noisy channel, they will correct GPS coordinates, which are converted to bits. When GPS coordinates are read in from the

system, they are immediately converted to bits. Each decimal place in the numbers returned by the GPS sensors is converted into a four-bit binary representation. The decimal place in this conversion is represented by four 1's. Six places after the decimal point are taken into account. Once this is done, the latitude and longitude binary representations are concatenated together into a vector. This vector is then used to create a "secure sketch." A secure sketch (ss) is the vector created from the GPS coordinates combined via a XOR operation with a valid LDPC codeword, which is a mapping of a word to a codeword so that it can be corrected. This codeword is specially created for the system to correct bit errors if necessary after transmission. Finally, this secure sketch is concatenated with a hash of the created vector and this final product is sent to the server to be stored. This process performs corrects errors and obscures the GPS coordinates in the database to ensure location privacy. We will now discuss what happens when the application tries to verify whether it is in range of a trusted location or not.

When the user tries to access the application a second time, the mobile application will then send an encrypted vector of the GPS coordinates to the server to be validated. When the vector reaches the server, it then has a XOR operation performed on it, which will give the server a codeword. This new codeword should be able to be corrected to the original codeword used to create the secure sketch. If this codeword is corrected to the correct and original codeword, this codeword is XOR'ed with the stored secure sketch. The result of this operation should result in the enrolled GPS location coordinates. The hash value of the corrected GPS location coordinates is compared with the hash value sent originally to the server. If the hash values match, the user is determined to be within a certain range of the original trusted location, and a message is sent from the server to the mobile device clearing the user to continue use of the application to carry out mobile banking applications. If the codeword cannot be corrected to the correct codeword,

the hash values will not match and the server will not allow the user to access the mobile banking application.

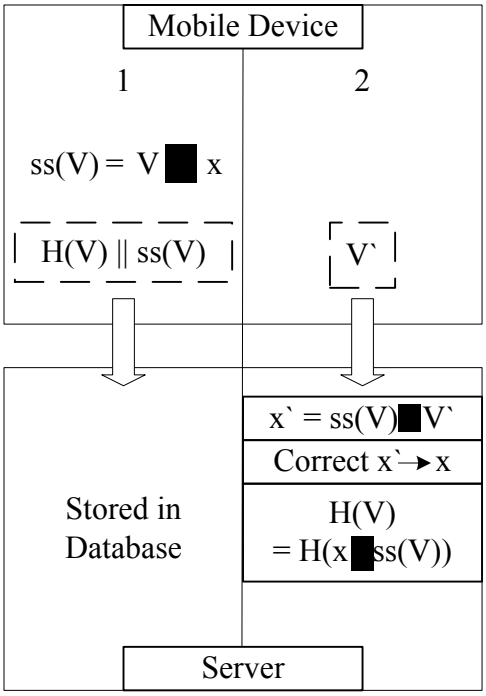

Figure 4. An LDPC representation

B. IMPLEMENTATION

The system described above was implemented and tested. The mobile device platform used was a Samsung Focus Flash with the Windows Phone 7.5 operating system. This mobile device was equipped with a GPS sensor, Wi-Fi, and mobile data connection. The system was implemented in two places. One was the application, which was implemented on the mobile phone in C#. The other was the server, which stored the GPS coordinates. This was comprised of a Windows Desktop Application written in C#, which was connected to a Microsoft SQL Server 2012 Database. The implementation was able to take GPS measurements and send them to the server, which was then able to validate its position within a certain range.

IV. RESULTS AND ANALYSIS

A. METHODOLOGY

To test the system described above, two procedures were carried out in an attempt to correctly test this system. The first procedure was to test the GPS sensors within the mobile device and their accuracy. This testing would answer a number of questions, including is the system even feasible. The second procedure was to build a mobile banking application which incorporated all of the features described above to create a prototype for testing.

GPS Accuracy Testing

A mobile application was developed which tested the accuracy of the GPS device within the mobile phone. This application was simple as it measured the current GPS coordinates and sent them via a TCP connection to a server to be stored. Two areas were designated as the test areas and several points were chosen within these areas to take GPS readings. One of these areas was indoor and one was outdoor. The outdoor area was a city with a population of about 65,000. It was a mountainous area, which made it a worst-case scenario for a user using this application requiring accurate GPS coordinates. The area also contained sections that were both urban and rural, allowing for a more diverse set of results. The weather was fair throughout the testing in this area, which could lead to further concern regarding unfavorable weather such as thunderstorms and snow. The indoor area was an office building with a long center hallway and five floors. Testing here was done on all sides of the building and on multiple floors. This was all done to determine the feasibility of the system as to whether or not the GPS could take accurate enough readings for the system to actually work, and how large the radius of a trusted location would need to be to work efficiently. The procedure for testing in these locations

involved walking to each designated point in our area in a specific order, and taking GPS readings at each point. This was done a total of ten times for each location. These readings were then stored on the server so that they could be analyzed in a table to determine the accuracy and range of the sensors.

Table 1 shows the comparison between the points measured by this application and the mobile phone, and the actual GPS coordinates, which were obtained using an online application [18]. As one can see in Table 1, some of the values in the table demonstrate that the GPS readings were very accurate in some locations, being off by only a few meters on average. However, some were off by around thirty meters on average as well. What can also be learned from the graph is that the indoor locations, while still usable for the application, averaged around thirty meters of inaccuracy, while the outdoor locations faired much better.

Table 1. Location Error for the System

Location Number (Outdoor)	**Mean Absolute Error (Meters):**	**Standard Deviation of Absolute Error (Meters):**
1	37	51
2	4	2
3	6	4
4	3	2
5	21	53
6	16	41
Location Number (Indoor)		
1	34	38
2	37	25
3	23	32
4	54	32
5	38	23

Simulated Banking Program

An application was developed which simulated a mobile banking program that measured GPS coordinates and tried to validate a user's location. It connected with a server written in C# which received the user's coordinates and determined if the user was in range of a trusted location. Example screenshots of this application can be seen in Figure 5. This application worked surprisingly well and was able to detect whether a user was within range reasonably well and allow a user to use the mobile application. This simple banking program also carried out mock banking operations such as depositing funds and making a withdrawal and transfer. A username and password were also required to use the application as it was assumed that all mobile banking applications would also use this standard security feature. As we can see in the center of Figure 5, the first time a user logs in they are asked to set their current location as a trusted location. The right side of this figure demonstrates an instance where the user is not measured to be within range of one of their trusted locations. Therefore, an email was sent to them so that they can authenticate themselves and choose to set this new location as a trusted one.

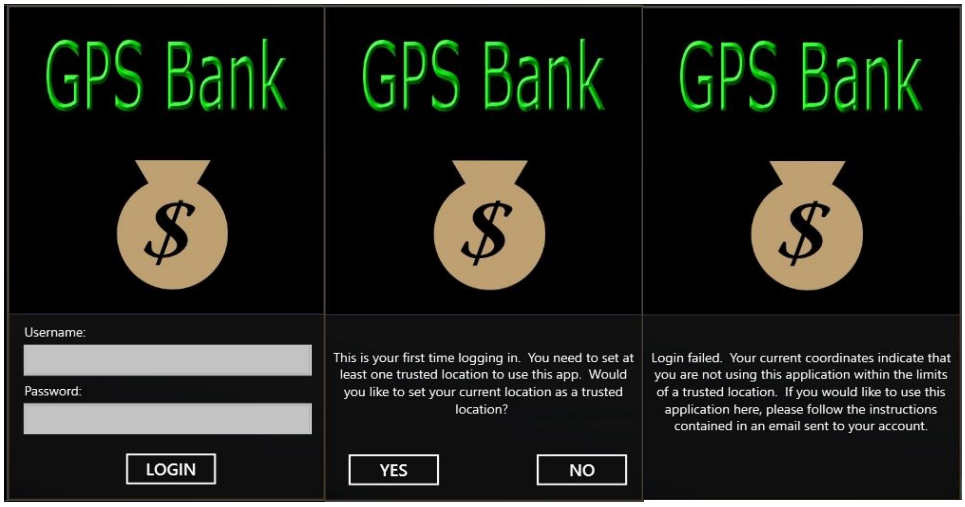

Figure 5. Examples of the mobile application's screens.

Many maps were also used to plot points and take measurements for accurate testing. Figure 6 gives an overall map of the area in which the outdoor testing locations were located. The red marker on the map, marked with a '1', is where the original trusted location was set. The immediate buildings surrounding this marker were an apartment complex. The rural neighborhood can be seen in the left side of this figure, which contained normal size houses and was relatively flat. In the bottom right hand side of this figure one can see a small mountain.

Figure 6. The outdoor mobile testing area [17].

In Figure 6, we can see a clear envisioning of what an acceptable radius would be for a trusted location. A big concern in location privacy is if any restrictions will be put upon the user to use the application, simply to maintain privacy and security. If the radius of a trusted location was too small, the user would not be able to comfortably move about their home or other trusted location to use their mobile banking application. Therefore, this roughly 150 meter radius was determined to be acceptable to our system as resembles the actual radius used for testing the GPS accuracies and mobile applications used in this system.

B. RESULTS

First, the GPS accuracy testing is discussed. In the initial GPS accuracy testing, some of the measured points had good accuracy, and some did not. Some readings were off by more than several miles, which raised concern about the legitimacy of the system.

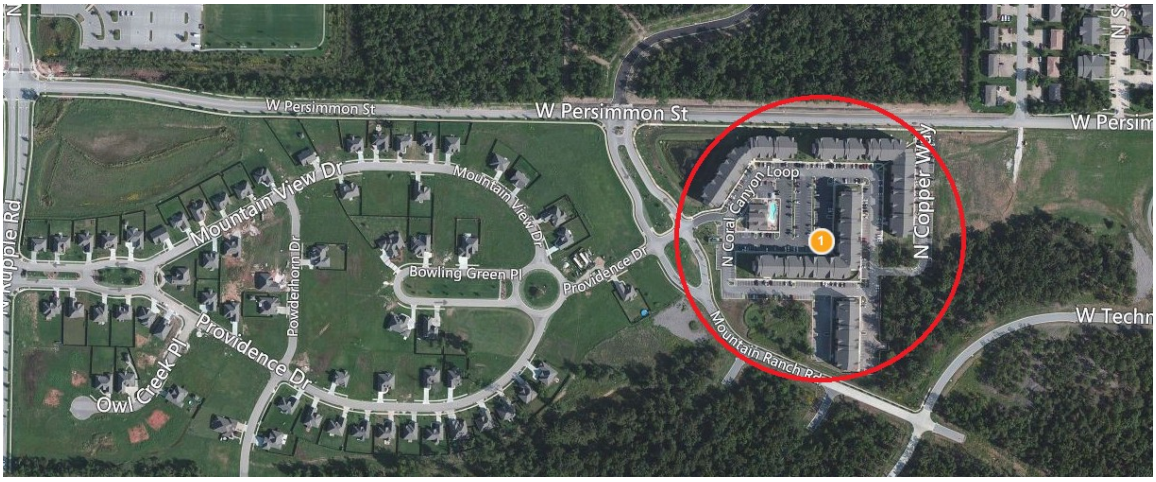

Figure 7. An example radius of a trusted location [17].

Much testing was done in several different areas, with ranges from a few hundred feet to around one square mile. In later rounds of testing for GPS accuracy, the accuracy improved, the reason for this will be explained in the next section. The results still demonstrated however, that the GPS sensors in the mobile device were not the most accurate, and could easily take measurements off by a few dozen meters as seen in Table 1.

The results showed that a user could set a trusted location, and subsequently log in with a username and password and use the application seamlessly with the benefit of location security. Mock transactions were made. The user was then able to walk out of range and be rejected for banking operations. As with the GPS measurements, sometimes the banking application failed to determine that the user was within range of a trusted location when they actually were.

However, this was the fault of the GPS sensor taking inaccurate measurements, not the application itself.

C. ANALYSIS

From the testing performed, two main ideas were garnered from the information. The first was that the accuracies being read in the initial GPS testing were much too coarse. Fortunately, most mobile devices contain two settings for GPS accuracy. One is the standard accuracy, and one is high accuracy. High accuracy uses more power, but is able to obtain much more accurate readings for our application. Therefore, once this setting was applied, the application become much more practical as the margin of error was reduced from several miles to several hundred feet. The second important piece of information which was discovered during testing was the desired range of a trusted location. Before testing, it was unclear what the radius needed to be as the authors were unsure of the accuracy of the GPS sensors of the mobile device. An ideal case was kept in mind, but the true accuracy of the system needed to be tested. After GPS accuracy testing, this radius was found to be about 0.001 degrees using the coordinate system. This gives the user a range of around 150 meters. This was concluded by the fact that the GPS sensors give back varying values after the third decimal place in the measurements and cannot be trusted.

V. CONCLUSIONS

A. SUMMARY

Mobile banking is becoming an increasingly important part of the banking industry today. As with any new technology, the need for security is great. Yet because mobile banking security involves a person's financial information, this need is even greater. The proposed solution describes a system which will add another form of authentication, a person's location, to better secure mobile banking applications. In this system, the fact that a user is normally within the same places each day is leveraged to use their GPS coordinates to verify their location. This set of coordinates is obscured using low density parity check, or LDPC codes and sent to the server, where it can be compared against for future application uses. LDPC codes also help to correct errors from inaccurate GPS coordinates. Overall, the system proposed here aims to increase security involving mobile banking while still maintaining location privacy.

B. CONTRIBUTIONS

If this thesis were to be fully implemented and tested to work across multiple platforms in multiple areas, it could lead to many different improvements in the mobile banking security area. The first of these is the more widespread and trusted use of mobile banking applications. If this system leads to a very successful and secure mobile banking system, users would feel more comfortable using mobile banking applications which implemented this system. Since the transfer of their financial information through public networks is always a large concern, this added security would be a large improvement and confidence builder for users. It would also lead to an increase in confidence in location privacy enabled applications as well. This could be

seen across not only many mobile banking applications but across other location enabled applications as well.

C. FUTURE WORK

This project has made several innovative contributions to this field, while also opening up many new doors and research opportunities. There are many aspects of this system which can be improved upon and added to. These additions could lead to a much more secure and efficient system. Some general examples of these things include improving the protocols used between the server and the mobile device. Also, safeguarding against spoofing would be a reasonable secure measure to take. As well as these, adding encryption to the system where LDPC codes are not entirely secure may help to fill in gaps in the security. All of these things would be improvements to the system, and could be added to the system with further research.

Another thing which can be done to improve the system is to test it with a variety of GPS sensors. These GPS sensors will all have different accuracies and will work with the proposed system differently. Considering the errors received on the phone described in the testing used for this system, it is expected that the system will need extensive testing with other GPS sensors for different phones. As well as this, using Android phones and the Apple IPhone will be useful or important? for testing as the final expected result of this system is to be able to use it successfully with every type of mobile device.

Finally, the most important future work project which can be done is to improve the implementation of LDPC codes. At the time of this writing, much of the work involving LDPC codes must be done offline, and not on the mobile device itself. This is due to factors, including battery power, complexity, and processing power. LDPC codeword generation is a complex process, and therefore, an implementation that is efficient and suitable for our system is not

widely available. A new implementation must be implemented in order to specifically suit the system. Power consumption is another concern, due to the fact that GPS sensors already consume significant power. In addition to this, adding a computationally complex coding scheme would only drain the battery further. Future work would involve implementing an efficient version of LDPC codes which could generate code words on the mobile device.

REFERENCES

[1] M.King. “Is Mobile Banking Breaking the Tyranny of Distance to Bank Infrastructure? Evidence from Kenya.” Internet: http://www.tcd.ie/iiis/documents/discussion/pdfs/iiisdp412.pdf, Oct. 2012 [Jan. 15, 2014].

[2] "What Is GPS?" Internet: http://www8.garmin.com/aboutGPS/, [Mar. 10 2014].

[3] M. Brain and T. Harris. "How GPS Receivers Work." Internet: http://electronics.howstuffworks.com/gadgets/travel/gps.htm, [Mar. 11 2014].

[4] S. Johnson. *Iterative Error Correction: Turbo, Low-Density Parity-Check and Repeat-Accumulate Codes*. Cambridge: Cambridge UP, 2010, pp. 34-118.

[5] M. Tinoosh. “Error Correction and LDPC Decoding.” Internet: www.csee.umbc.edu/~tinoosh/cmpe691/slides/ldpc-decoding-v2.ppt, [Mar. 16 2014].

[6] M.Andersen, M. Kjærgaard, and K. Grønbæk. "The SITA Principle for Location Privacy– Conceptual Model and Architecture." in *Proc. International Conference on Privacy and Security in Mobile Systems*, 2013.

[7] M. Shirali-Shahreza, and M. Shirali-Shahreza. "Mobile Banking Services in the Bank Area." in *Proc. SICE*, 2007.

[8] C. Chang, J. Yang, and K. Chang. "An Efficient and Flexible Mobile Payment Protocol." in *Proc. Genetic and Evolutionary Computing (ICGEC)*, 2012, pp. 63-66.

[9] M. Elkhodr, S. Shahrestani, and K. Kourouche. "A Proposal to Improve the Security of Mobile Banking Applications." in *Proc. ICT and Knowledge Engineering (ICT & Knowledge Engineering),* 2012, pp. 260–265.

[10] M. Gordon, and S. Sankaranarayanan. "Biometric Security Mechanism in Mobile Payments." in *Proc. Wireless And Optical Communications Networks (WOCN)*, 2010.

[11] C. Tsai, C. Chen, and D. Zhuang. "Secure OTP and Biometric Verification Scheme for Mobile Banking." in *Proc. Mobile, Ubiquitous, and Intelligent Computing (MUSIC),* 2012, pp. 138–141.

[12] S. Panjwani, and E. Cutrell. "Usably Secure, Low-Cost Authentication for Mobile Banking." in *Proc. Proceedings of the Sixth Symposium on Usable Privacy and Security*, 2010.

[13] M. Paik. "Stragglers of the Herd Get Eaten: Security Concerns for GSM Mobile Banking Applications." in *Proc. Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, 2010.

[14] B. Cao and Q. Fan. "The Infrastructure and Security Management of Mobile Banking System." in *Proc. International Conference on E-Product E-Service and E-Entertainment*, 2010.

[15] Dewri, Rinku, Wisam Eltarjaman, Prasad Annadata, and Ramakrishna Thurimella. "Beyond the Thin Client Model for Location Privacy." in *Proc. International Conference on Privacy and Security in Mobile Systems*, 2013.

[16] J. Brassil, and Pratyusa K. Manadhata. "Proving the Location of a Mobile Device User." in *Symposium Virginia Tech Wireless,* 2012.

[17] “Google Maps.” Internet: www.maps.google.com, [Feb. 1, 2014].

APPENDIX A. - ADDITIONAL FIGURES AND TABLES

Figure 8. Indoor Testing Area [17].

Table 2. Indoor Testing Area - Actual Coordinates

Location:	Actual Latitude:	Actual Longitude:
1	36.065980000000000	-94.173457000000000
2	36.066501000000000	-94.173818000000000
3	36.066410000000000	-94.174079000000000
4	36.065712000000000	-94.173981000000000
5	36.065642000000000	-94.173517000000000

Table 3. Indoor Testing Area Measured Coordinates

Latitude:	Longitude:
36.066199302673300	-94.173841476440400
36.066441535949700	-94.173196792602500
36.066946545649400	-94.174118125898900
36.066836742717800	-94.174116784794400
36.065638256292800	-94.173481436534000